## CLIN 021 - SECURITY ADMINISTRATION SERVICES - MAINFRAME ~~SECURITY,~~ AUTHENTICATION, ROLE MANAGEMENT, AND ACCESS CONTROLS

### 1. OVERVIEW

The objective is to obtain security analysis and engineering services, including subject matter expert support, necessary for managing system security controls, authentication services, and role based software governing access to enterprise infrastructure and mainframe systems, in support of the Security Division, Systems Security Branch (SD/SSB) of the National Information Technology Center (NITC).

### 2. SCOPE/DUTIES

The specific tasks to be supported and completed include, but are not limited to, those identified below.

a) The administration, monitoring, operation, analysis, maintenance, and reporting of the mainframe authentication, authorization, and access controls system (currently: CA Access Control Facilities 2 (ACF2) and IBM Resource Access Control Facility (RACF)).
b) The contractor shall use Vanguard's VSS, ~~and~~ the Eberhart Klemens Co. and IBM Z Secure access rule clean up suite of tools to perform their access control clean up tasks.
c) The contractor shall use the Computer Associates, CA Audit system and other supporting mainframe utilities for monitoring, diagnostics, and analysis.
d) The contractor shall execute native ACF2 / RACF commands utilizing GUI and panel-drive interfaces to administer ACF2 / RACF.
e) Establish and maintain ACF2 and RACF logon IDs.
f) Establish and maintain ACF2 and RACF security rules and parameters.
g) The contractor shall integrate a Role Based Access Controls (RBAC) process using Identity Management software.
h) The contractor shall work with midrange, mainframe ~~system~~ and network engineers to strengthen the security posture of enterprise systems using Authentication, Authorization, and Audit (AAA) and Public Key Infrastructure (PKI) services.
i) The contractor shall perform incident, problem, change, release, and configuration management following data center procedures.
j) The contractor shall work the service request ticket queues for access, accounts, roles, digital certificates, systems integration, and troubleshooting on hosted systems.
k) The contractor shall perform account management tasks on enterprise infrastructure, Microsoft, Unix, and mainframe systems.
l) The contractor shall perform access control tasks on enterprise infrastructure, Microsoft, Unix, and mainframe systems.
m) The contractor shall perform system, security, and application log and reports reviews following established procedures.
n) The contractor shall follow NITC's internal documented standards, processes, and procedures on Mid-Range and Mainframe platforms which govern authentication, user account management and system access controls.

o) The contractor shall document all aspects of the system for installation, daily operations, disaster recovery, and federal certification and accreditation requirements in the required format.
p) The contractor shall provide statistical reporting to illustrate enterprise security data.
q) The contractor shall follow NITC approved guidance from NIST.GOV Special Publications (Series: 800), USDA Departmental Directives (Series: 3100, 3300, 3400, 3500, 3600) and other applicable regulations and guidance for system controls in support of daily duties and audit requirements.
r) The contractor shall draft, review and submit security policy, standards, process, procedures, and system documentation.
s) The contractor shall support the technical evaluation and testing of security tools.
t) The contractor shall conduct security system and documentation reviews for managed systems.
u) The contractor shall analyze systems performance of new and existing equipment.
v) The contractor shall provide knowledge transfer to other team members, as well as to government personnel.

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent experience (with in the last ~~12~~ 24 months) on Mid-Range platform experience.
b) Experience with Active Directory / LDAP is preferred.
c) Experience with Identity Manager on the mainframe is preferred.
d) Experience as an application developer/programmer is preferred.

## 4. ADDITIONAL INFORMATION AND REQUIREMENTS

The Government is providing the historical information below to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements.

| Number of FTE | General/Estimated Skill Level |
|---|---|
| 2 | intermediate |
| 1 | Junior (NEW) |

## CLIN 022 - SECURITY ENGINEERING - ASSESSMENT SERVICES

### 1. OVERVIEW

The objective is to obtain technical support for security assessment tools, vulnerability scanning tools, and penetration testing to support the Security Division, Information Security Branch (SD/ISB). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

### 2. SCOPE/DUTIES

a) Install, administer and manage the NITC vulnerability assessment environment.
b) Monitor Remedy ticket queues for the Information Security Branch (ISB) Assessment team and processes/works incidents and change request tickets as they are assigned to ISB Assessment.
c) Perform monthly and ad-hoc scans across the NITC network environment.
d) Document all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
e) Provide statistical reporting to illustrate security posture and continuous improvements.
f) Participate in the creation, review and enforcement of security policy, procedures and system documentation.
g) Evaluate, make recommendations, implement or disseminate IT security tools, procedures and practices to protect organizational systems.
h) Provide knowledge transfer to team members, to include government counterparts.

### 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Detailed experience and understanding of Microsoft, Linux and UNIX operating systems.
c) Experience in Information Security.
d) Experience with at least one of the following scanning technologies: eEye Retina, Rapid7 Nexpose, Metasploit, Core Impact, Nessus, dbProtect, or Appdetective.
e) Thorough understanding of the following security technologies:
   - Firewalls/Routers/Switches
   - Vulnerabilities/Risks/Threats
   - Cyber Incident Response techniques

# CLIN 023 - SECURITY ENGINEERING – MONITORING, DETECTING AND ANALYSIS SERVICES

## 1. OVERVIEW

The objective is to obtain technical support for intrusion detection/prevention systems, security incident and event management (SIEM) tools, and other various network perimeter defense solutions, in support of the Security Division, Information Security Branch (SD/ISB). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

## 2. SCOPE/DUTIES

a) Installs, administers and manages the NITC Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS), Security Incident and Event Manager (SIEM), Wireless Intrusion Prevention Systems (WIPS) and Host-based Intrusion Detection systems (HIDS/HIPS).
b) Monitors Remedy ticket queues for Information Security Branch (ISB) Monitoring Detecting and Analyzing (MDA) team and processes/works incidents and change request tickets as they are assigned to ISB MDA.
c) Performs Incident Response activities by following the NITC Incident Response procedures in the event that a Cyber Incident occurs.
d) Documents all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
e) Provides statistical reporting to illustrate security posture and continuous improvements.
f) Participates in the creation, review and enforcement of security policy, procedures and system documentation.
g) Evaluates, makes recommendations, implements or disseminates IT security tools, procedures and practices to protect organizational systems.
h) Provides knowledge transfer to team members, to include government counterparts.

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Detailed experience and understanding of Microsoft, Linux and UNIX operating systems.
c) Experience with a Security Incident and Event Management (SIEM) tool.
d) Experience in Information Security.
e) Experience with one of the following IDS/IPS technologies: SourceFire, McAfee, HP TippingPoint, Cisco, and Snort.
f) Thorough understanding of the following security technologies:
   - Firewalls/Routers/Switches
   - Packet Capture (PCAP) analysis
   - IT System Forensics

## CLIN 024 - SECURITY ENGINEERING - NETWORK ACCESS CONTROL SERVICES

### 1. OVERVIEW

The objective is to obtain technical support for firewalls, remote access solutions, and other various network perimeter defense solutions in support of the Security Division, Information Security Branch (SD/ISB) at the National Information Technology Center (NITC). This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors.

### 2. SCOPE/DUTIES

a) Installs, administers and manages the NITC firewalls, Access Control Lists (ACL), Virtual Private Network (VPN) systems and Web Proxies.
b) Monitors Remedy ticket queues for Information Security Branch (ISB) Network Access Control (NAC) team and processes/works incidents and change request tickets as they are assigned to ISB NAC.
c) Documents all aspects of the system for daily operations and disaster recovery, in addition to adherence of federal certification and accreditation requirements.
d) Provides statistical reporting to illustrate security posture and continuous improvements.
e) Participates in the creation, review and enforcement of security policy, procedures and system documentation.
f) Evaluates, makes recommendations, implements or disseminates IT security tools, procedures and practices to protect organizational systems.
g) Provides knowledge transfer to team members, to include government counterparts.

### 3. EXPERIENCE AND EXPERTISE REQUIREMENTS:

a) Experience in networking design and concepts to include TCP/IP, switching, routing, firewalls, virtual route forwarding and VLANs.
b) Experience in Information Security.
c) Experience with two of the following firewall technologies: Juniper/Netscreen, Cisco, Checkpoint, Fortinet, Palo Alto.
d) Thorough understanding of the following security technologies:
   - Intrusion Detection/Prevention Systems (IDS/IPS)
   - Log Management and Security Incident and Event Management (SIEM)
   - Virtual Private Network (VPN) Remote Access
   - Web Content Filtering / Web Proxy

## CLIN 025 - SENIOR APPLICATIONS ENGINEERING SERVICES

### 1. OVERVIEW

The objective is to obtain technical support services required to execute the transition of USDA and non-USDA customer business applications to the USDA Enterprise Data Centers (EDC).

In 2010, the Office of Management and Budget initiated the Federal Data Center Consolidation Initiative (FDCCI). The focus of the FDCCI is to reduce the number of computer rooms, the amount of energy consumption, and to consolidate business applications into designated Agency EDCs.

The contractor will be required to focus on transitioning business applications and will be the primary NITC point-of-contact between the customer and applicable EDC representatives. The contractor will be required to make contact with NITC customers, technical staff, business partners, management, and internal and external auditors.

### 2. SCOPE/DUTIES

The specific tasks to be supported by the contractor include, but are not limited to, those listed below.

a) The contractor shall complete all task activities in accordance with NITC service offerings, tools, and best practices.
b) Meet with customers as required gaining a sufficient understanding of their business application environment (e.g., critical application production timeframes), document system requirements, and aligning to available NITC service offerings.
c) Develop .customer application inventories to capture operating systems, application languages, databases, storage protocols and volume, customer and administrator access methods, application architecture, and application interdependencies.
d) Utilize NITC server and desktop discovery tools and resulting information to assist in the development of EDC hosting estimates
e) Utilize NITC server and desktop discovery tools and resulting information to develop EDC target architectures.
f) Gain an understanding of customer application test plans and assist in test plan execution.
g) Ensure customer access requirements to application target architecture are operational and meet customer requirements.
h) Execute, directly with customer, application test plans and maintain primary point-of-contact role between customer and applicable EDC representatives to minimize issue resolution timeframes.
i) Ensure that customer test plans are successful, resolve related issues, and coordinate with EDC Engineers on any final application architecture changes.
j) Provide continued support to ensure customer application transitions are successfully completed.
k) Act as liaison between customer and applicable NITC staff to answer customer questions.

l) Make optimal service design recommendations to customers, consistent with common service offerings.
m) When required, build network diagrams for customer environments hosted at the NITC.
n) Create and submit build documents on behalf of customers.
o) As required, the contractor shall monitor and track progress of customer build requests.
p) Review and provide feedback on service documentation (catalog, appendices, and architectural standards).

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Well-rounded skills in networking, security, storage solutions, disaster recovery as well as a more detailed skill set in working with operating systems, applications and databases.
b) Implementing Open Systems Interconnection model architecture which includes routing, switching, VLANs, load balancing and traffic analysis.
c) Security – firewall, access controls, Active Directory and application vulnerability scanning.
d) Storage – Storage Area Network, Network Attached Storage, large data transfers and back-up/recovery.
e) Disaster Recovery Strategies – Active-Active and Active-Passive.
f) Operating Systems – Windows, Linux, AIX, HP-UX, Solaris and virtualization technologies.
g) Applications and Database – Application design and architecture in n-tier environments. Migration of applications utilizing server and desktop discovery tools and develop/execute application test plans. Required application environments and databases are, but not limited to, J2EE, .NET, IIS, Apache, Oracle, MS SQL and DB2

## CLIN 026 - SERVER AUTOMATION TOOL SUPPORT SERVICES

### 1. OVERVIEW

The objective is to obtain Server Automation Tool Support Services for Open Systems (UNIX) and Microsoft (WINDOWS SERVER) computing platforms at the National Information Technology Center (NITC). The NITC currently utilizes BMC Server Automation~~, BMC Orchestrator,~~ and BMC Advanced Reporter. The Microsoft and Open systems platforms will be referenced as "midrange" in the remainder of this document**.**

### 2. SCOPE/DUTIES

The Contractor shall provide Server Automation Tool Support Services support for NITC. The specific tasks to be supported and completed include, but are not limited to, those identified below.

a) Install, test, configure, customize, and maintain the server automation tools. This includes upgrades as well as agents on servers.
b) Create, schedule, perform, maintain and monitor server automation jobs.
c) Support patching requirements as required.
d) Support the automation of system provisioning
e) Create, execute, troubleshoot, and maintain optimized automation scripts.
f) Develop, execute and maintain standard and custom reports for ongoing metrics and data calls.
g) Collaborate with BMC Remedy, Atrium Discovery and Dependency Mapping (ADDM), Atrium Configuration Management Database (CMDB), and BMC ProactiveNet Performance Monitoring (BPPM) teams to support integration efforts ~~using BMC Orchestrator~~.
h) Create, execute, troubleshoot, and maintain optimized custom scripts for managing security compliance.
i) Perform hardening of systems per NITC, OCIO Cyber-Security, and Departmental Policies, Standards, Regulations, and Notices, to include security monitoring and updating of certification/accreditation procedures.
j) Confirm that server automation environment is backed up as required and ensure disaster recovery readiness.
k) Make recommendations for server automation system performance improvements.
l) Troubleshoot overall system problems and identify/resolve problems.
m) Manage the role-based access control (RBAC) security model of NITC and customer access into the server automation console.
n) Document and perform changes and resolve incidents and problems using NITC's Configuration Management Tools and Systems.

### 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent (within the last 12 months) experience with BMC Server Automation ~~and Orchestrator~~ required, including installation, configuration, operation, upgrading, and providing maintenance of the product.
b) Systems administration techniques on IBM AIX, Microsoft Windows Server, Oracle Solaris, and RedHat Linux operating systems, operating in a complex, diverse, enterprise environment, is preferred.
c) Virtualization techniques such as IBM LPARs, Solaris Zones, and VMware hypervisor, is preferred.

# CLIN 027 - STORAGE ADMINISTRATION SERVICES

## 1. OVERVIEW

The objective is to obtain technical support for storage administration assistance to the Information Services Division, Storage Management Branch (ISD/SMB), National Information Technology Center (NITC). The contractor shall perform various duties, particularly in the technical areas of Storage Area Network (SAN) administration, Network Attached Storage (NAS) administration, Cloud Storage, Software-Defined Storage (SDS), Virtual Tape administration, and Open Systems Backup administration.

This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors. Contractor shall follow SMB hardening guides and storage procedures.

## 2. SCOPE/DUTIES

The SMB currently operates storage environments in six data centers (Kansas City, MO; Beltsville, MD; St Louis, MO; Fort Collins, CO; Fort Worth, TX; and Salt Lake City, UT). Storage administration duties shall be performed remotely for Beltsville MD. The storage solutions operated by NITC are based on Brocade switch technology, Hitachi Data Systems (HDS) enterprise disk technology, SUN/StorageTek (STK) enterprise tape technology, ~~Symantec~~Veritas NetBackup software, EMC Data Domain, and EMC enterprise and modular disk technology (with a few sites having SUN disk technology for archiving), NetApp appliances, Ceph for cloud storage, and ~~IBM Virtual Tape~~Luminex System for mainframe virtual tape.

All required services are to be provided by the contractor and shall comply with applicable standards, policies, and procedures. The Contractor shall implement security controls, create/update documentation, to include configuration and automated processes, and develop project plans/tasks lists. Categories of services to be provided include, but are not limited to, the following:

- Storage administration services
- Storage design and architecture
- Storage virtualization
- Storage maintenance
- Storage performance evaluation and analysis

Specific tasks include, but are not limited to, those identified in the subsequent paragraphs.

a) Installing and configuring software; completing backup and restore requests; performing storage allocations; adding clients to backup policies; decommissioning systems; configuring media and master servers/drives/robots; performing updates/upgrades/patches to hardware/software/firmware; troubleshooting issues; monitoring systems; and reporting, etc.

b) Development and maintenance of required documentation. The documentation includes, but is not limited to, the following: SAN Billing Table, configuration documents, NetBackup documents, SAN administration request form, etc.
c) Operation of all aspects of storage administration tools and products including installation, configuration, operation, upgrading, and providing maintenance of products.
d) Scheduling, building, troubleshooting automation jobs, including compliance and remediation jobs, auditing jobs, package installation, and provisioning jobs.
e) Installing, configuring, upgrading, maintaining, and creating reports using reporting tools.
f) Monitoring and recommending improvements for performance of storage products.
g) The contractor shall perform the following frequently recurring project tasks and special projects that incorporate the duties described above.
   - Disk Storage administration and support – Occurs daily
   - SAN Switch administration and support – Occurs daily
   - SAN and NAS Solution administration and support – Occurs daily
   - Tape Storage administration and support – Occurs daily
   - ~~Symantec~~Veritas NetBackup administration and support – Occurs daily
   - Replication activities and support – Occurs daily
   - Oral and written communication with NITC management as well as internal and external customers – Occurs daily
   - Disaster Recovery Testing Activities – As required, approximately 1-2 times per month
   - Disaster Recovery Planning and Documentation – As required.
   - NITC Vital Records Documentation – As required unless specifically assigned documentation tasks, then daily.
   - Weekly Activity Reporting – Occurs weekly
   - Configuration Management and Change Control Procedures – As required, approximately 1-2 times per week, includes specific storage documents

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

The contractor shall have the following general experience and expertise:

- Specialized experience with enterprise storage solutions.
- Experience with storage administration techniques on enterprise class storage, mid-tier storage, and direct attached storage.
- Familiar with virtualization techniques such as IBM LPARs, Solaris Zones, and VMware.
- Familiar with requirements for telecommunication.
- Working knowledge of various protocols such as iSCSI, NFS, CIFS, etc.

The contractor shall have the following specific experience and expertise:

- SAN Disk Technologies:
  - HDS enterprise disk technology (e.g. ~~9980,~~ USP, USP-V, VSP, and G series, etc.) provisioning and performance management in a SAN storage environment.
  - Remote and In-System Replication configuration and support.
  - Hitachi Universal Replicator (HUR), and subsystem architecture and configuration.

- IBM ~~(DS8000),~~ EMC (DMX, Data Domain, and Clariion), and other industry leading disk technologies.
- Working knowledge of EMC ECC.
- Installation and upgrade the ECC console.
- Utilization of Performance Monitor and in depth analysis of EMC devices.
- Working knowledge of EMC replication software, SRDF.
- Working knowledge of setup and administration of mirror pairs between remote sites.

- Cloud Technologies:
  - Cloud storage technologies such as Ceph to manage vast amounts of data and applications with different storage interface needs.
  - Knowledgeable of Ceph's Reliable Autonomic Distributed Object Store (RADOS).

- SDS Technologies:
  - Implementation and management of software-defined storage solutions to support dynamic applications and workloads in virtualized environments.

- SAN Switch Technologies:
  - Brocade SAN switch technology operation, provisioning, and support.
  - Familiar with SAN channel extension technologies used for remote data replication purposes.

- SAN Tape Technologies:
  - SUN/STK automated tape technologies (e.g. ~~9310,~~ L700, SL8500, etc.).
  - STK Automated Cartridge System Library Software (ACSLS).
  - ~~9840 and~~ LTO tape drive technology.
  - Oracle Hierarchical Storage Manager (known formally as SUN Storage Archive Manager File System (SAMFS) archive solution.

- NAS Technologies:
  - NetApp Appliance technology (e.g. 6200, 3020, v3140, 80xx, etc.)
  - vFilers
  - Common Internet File System (CIFS)
  - Network File System (NFS)
  - Snap Manager for Oracle

- Virtual Tape Technologies:
  - Virtual Tape technology (e.g. Data Domain Appliances for Open Systems and Luminex for mainframe, IBM Virtual Tape System (VTS) for mainframe), and replication including HUR, NetBackup~~,~~ Automatic Image Replication (AIR), and/or VTS Grid.

- Open Systems Backup Technologies:
  - ~~Symantec~~Veritas NetBackup installation, administration, maintenance, and support in an enterprise environment including Microsoft Windows, Sun Solaris, and IBM AIX clients and media servers.

- Backup and Archive Technologies:
  - Oracle Hierarchical Storage Manager (Oracle HSM – known formally as SAMFS) installation, administration, maintenance, and support in an enterprise environment.

- Reporting Technologies:
  - NetApp OnCommand Insight (OCI) – installation, administration, maintenance, and support reporting capability and dashboard to manage our multivendor IT storage infrastructure.
  - APTARE – installation, administration, maintenance, and reporting for open system backup infrastructure.

# CLIN 028 - SYSTEMS ADMINISTRATION SERVICES

## 1. OVERVIEW

The objective is to obtain systems administration support for physical and virtual operating systems utilizing MS Windows Server, Open Systems (UNIX – IBM AIX, RedHat Linux, and Oracle Solaris) and VMware based operating environments, supporting the Systems Engineering Division/Open Systems Branch (SED/OSB), the Systems Engineering Division/Windows Systems Branch, and limited support to the Infrastructure Operations Division, Systems Network Control Center (SNCC). These platforms will be referenced as mid-range in the remainder of this document. This may require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors. The Contractor shall provide IT support to a variety of mid-range systems, operating 24x7x365, and running a variety of applications.

## 2. SCOPE/DUTIES

The Contractor shall provide mid-range platform systems administration support on the mid-range platform servers located at the NITC locations, and remote support to other sites may also be required. The mid-range platform system administration support task requirements will include, but are not limited to, the following:

a) Design solutions to complex problems and provide solutions.
b) Troubleshoot overall system problems and identify/resolve problems in a fast paced environment.
c) Analyze system logs, and identify and remediate issues with systems.
d) Install, test, configure, customize, and maintain various server operating systems and associated software utilizing physical and virtual hardware. Utilize automated provisioning techniques to deploy new systems and software.
e) Set-up and configure complex networking configurations, Transmission Control Protocol/Internet Protocol (TCP/IP) networking.
f) Create, maintain, and execute scripts to perform routine maintenance.
g) Perform hardware maintenance of underlying server infrastructure including, but not limited to, replacing hard disks, fans, cpu/memory, i/o cards, and updating firmware.
h) Perform patch/fix research and operating system software upgrades through service packs and other software bundling methodologies. The contractor shall use current NITC patching techniques and automated patching products used at the NITC.
i) Utilize volume management techniques to create, maintain, expand, and shrink file systems; monitor performance of the file systems; and utilize RAID techniques and practices for availability and performance.
j) Utilize system tools to monitor performance, capacity, availability and perform operating system tuning.

k) Configure, customize, and optimize fail-over clustering or other high availability solutions.
l) Maintain and perform operating systems security:
   - Harden systems per NITC, OCIO Cyber-Security, and Departmental Policies, Standards, Regulations, and Notices. Security monitoring and updating of certification/accreditation procedures.
   - Add and remove local user accounts as necessary.
   - Address and resolve security vulnerabilities related to operating system software.
   - Add and remove EDC/AD domain user accounts and roles as necessary.
m) Maintain customer access to the systems and provide user with technical support.
n) Schedule, perform and maintain backups (including restoration) to facilitate data integrity, data storage and backup/recovery procedures, as required.
o) Document and perform changes and resolve incidents and problems using NITC's Configuration Management Tools and Systems.
p) Utilize server automation tools provided by NITC.
q) Provide knowledge transfer documentation to the Government as required.

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

Relevant experience, within the last 24 months, for each technical subject area (AIX, Linux, Solaris, VMware, Windows Server, and OpenStack).

## 4. ADDITIONAL INFORMATION

The Government estimates that varying levels and types of requisite skill sets will be required to complete the stated requirements. The Government is providing historical information to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements.

| Product Area | Estimated Staffing Level |
|---|---|
| AIX | 1 |
| LINUX | 4 |
| SOLARIS | 3 |
| VMware | 2 |
| Windows Server | ~~6~~3 |
| ~~SA in the SNCC~~ | ~~1~~ |
| OpenStack | 1 |
| ~~Linux/Open Stack~~ | ~~1~~ |

## CLIN 029 - SYSTEMS MONITORING ADMINISTRATION SERVICES

### 1. OVERVIEW

The objective is to obtain administration and support for systems monitoring utilizing HP OpenView, XYMON, BMC ProActiveNet Performance Management (BPPM), and Microsoft's System Center Operation Manger (SCOM) at the National Information Technology Center (NITC). The contractor shall manage the various Systems Monitoring Administrator duties within the Infrastructure Operations Division, Service Operations & Support Branch, Availability and Monitoring Team. Administrators shall also support other branches within NITC. This will require making contacts with NITC customers, technical staff, business partners, management, and internal and external auditors. The Contractor shall provide Information Technology (IT) support to a variety of monitoring systems, operating 24x7x365, and running a variety of applications. Teamwork, coordination, documentation, and security are critical aspects of success in performing the tasks.

### 2. SCOPE/DUTIES:

The Contractor shall provide administration on the monitoring systems located at the NITC locations, and remote support at other sites may also be required. The contractor duties shall include, but are not limited to, the following:

a) Install, operate and maintain HP OpenView applications in an enterprise environment, including the Business Availability Center, HP OpenView agents, and the Business Process Monitor components.
b) Install, operate and maintain the XYMON monitoring application in an enterprise environment.
c) Install, operate and maintain BMC ProActiveNet Performance Management (BPPM) applications in an enterprise environment.
d) Install, operate and maintain Microsoft's System Center Operation Manger (SCOM) application in an enterprise environment.
e) Troubleshoot overall system problems and identify/resolve problems.
f) Analyze system logs and identify potential issues with systems.
g) Install, test, configure, customize, and maintain various operating systems and associated software.
h) Perform patch/fix research and application software upgrades through service packs and other software bundling methodologies.
i) Performance/Capacity/Availability Monitoring and Operating System Tuning.
j) Configure, customize, and optimize fail-over clustering or other high availability solutions.
k) Schedule, perform and maintain backups to facilitate data integrity, data storage and backup/recovery procedures.
l) Maintain customer access to the systems and provide technical support to users.
m) Document changes, incidents, and problems using NITC's Configuration Management Tools and Systems.
n) Provide knowledge transfer documentation to the Government as required.

## 3. EXPERIENCE AND EXPERTISE REQUIREMENTS

a) Recent experience (within the last year) with HP Open View, XYMON, BMC ProActiveNet Performance Management (BPPM), SCOM.
b) Recent experience (within the last year) with scripting in VB, Perl, WMI and Shell.
c) Recent experience (within the last year) with generating reports with HP Open View, XYMON, BMC ProActiveNet Performance Management (BPPM), SCOM.
d) Recent experience (within the last year) with the setup of new monitoring in HP Open View, XYMON, BMC ProActiveNet Performance Management (BPPM), SCOM.

## 4. ADDITIONAL INFORMATION

The Government is providing historical information to illustrate the types of skill sets and the level-of-effort in terms of Full-Time-Equivalent (FTE) positions that have been utilized to support past requirements. Historically, the requirements have been satisfied via the utilization of approximately three FTE positions staffed at an estimated/general level of intermediate.

## CLIN 030 – ENTERPRISE PORTFOLIO AND CLOUD SUPPORT

## 1. OVERVIEW

The Business Development Manager within the Service Portfolio Branch manages the portfolio suite of technology services, and accompanying business processes that enable the United States Department of Agriculture (USDA) to achieve its goals and objectives of eGovernment, leveraging its investments and delivering government services in a more citizen-centric manner.

The services offered by the National Information Technology Center (NITC) Enterprise Data Center (EDC) are enterprise-wide. Department, Agency, or Federal eGovernment initiatives can leverage these services. USDA Agencies and initiatives do not have to create their own technology solutions and standards and can instead utilize the NITC EDC centralized service offerings to support their business requirements and thus avoid the high cost and high learning curve of operating these solutions independently.

## 2. SCOPE/DUTIES

a) IT Service Architecture. The contractor shall support tasks including, but not limited to, the following:
   i. Participate in identifying and prioritizing the next steps for the technical environments to include Government and Commercial Cloud Services. As agency use increases, components of the architecture are upgraded, and new requirements surface, changes to the service offering may be necessary to ensure that the technical environments, the application support as well as the financial impact are fair, equitable and functioning as expected. Any deviations from these service scopes will need to be identified as early as possible, planned and tracked to implementation.
   ii. Identify and manage new services offerings via Service Development Life Cycle (SDLC) best practices.
   iii. Plan support of and integration with any new service offerings, such as collaboration or records management. This includes discussions with NITC, other Office of Chief Information Officer (OCIO), or industry technical and business process teams to determine the necessary steps to support new offerings such as identifying hardware and software components, identifying required customization to meet customer or agency requirements, and ensure best value to the Government is developed in accordance with best practices.
   iv. Develop technical and business process standards for all architected environments/services. These standards shall follow best practices and support the NITC architecture both Government and Commercial.

b) Cloud Broker Support. As the USDA Cloud Broker, the NITC will have many unique functions that will need to be supported to ensure the successful deployment and management of cloud based service activities. The NITC requires additional support to be used to facilitate the on-going support and performance of these critical mission cloud functions. The contractor shall support tasks including, but not limited to, the following:

i. Architect and engineer new cloud services: The contractor shall support NITC's cloud service portfolio by enhancing existing cloud service offerings and developing and implementing new cloud services.
ii. Develop and maintain NITC cloud policy & guidance: The contractor shall provide support of cloud service policy and guidance. The contractor shall also interface with other USDA staff to assist with the development of department-wide policy as well as assist with cloud oriented government information requests.
iii. Lead cloud service development and planning activities: The contractor shall lead NITC cloud meetings and initiatives, as required. The contractor shall provide service assessments and guidance.

c) Service Level Management Support. NITC's Service Development Manager has oversight responsibility for NITC's Service Level Management (SLM) Program. The contractor shall support tasks including, but not limited to, the following:
   i. SLM Program establishment and continuous improvement. The contractor shall provide support for the establishment of the NITC SLM Program.
   ii. Develop and maintain NITC SLM documentation. The contractor shall provide support of SLM documentation creation and maintenance for NITC's Government cloud services, NITC staff, and consumers of NITC services. The contractor shall meet with technical subject matter experts, NITC customers, and industry SLM best practice forums in order to ensure NITC's SLM program and supporting documentation remain state-of-the-art.
   iii. Lead SLM activities: The contractor shall lead NITC SLM meetings and initiatives.
d) Service Development Life Cycle Support. The contractor shall support tasks including, but not limited to, the following:
   i. Service Development. The contractor shall provide assistance in developing new services for NITC Service Portfolio inclusion. The contractor shall lead meetings and working sessions with NITC and industry technical subject matter experts to gain an understanding of new service offerings. The contractor shall lead efforts to assess USDA and NITC customer demand for any proposed new services. After assessing sufficient demand, the contractor shall complete a service development life cycle analysis for the proposed new service.

**EXPERIENCE AND EXPERTISE REQUIREMENTS**

a) Experience with overall enterprise data center services life cycle development as well as the development and maintenance of service catalogs, in support of the organizational mission.
b) Microsoft Project.
c) Microsoft PowerPoint.
d) Technical knowledge of state-of-the-art and emerging cloud service offerings.
e) ITIL.
f) Working knowledge of industry best practices applicable to SLM.

## 3. PERFORMANCE STANDARDS / ACCEPTABLE QUALITY LEVELS / INCENTIVE / DISINCENTIVE

| Performance Requirement | Performance Standard | Acceptable Quality Level (AQL) | Incentive/Disincentive | Inspection Method |
|---|---|---|---|---|
| Product Management Analysis Deliverables and Tasks | ▪ 100% of applicable service offerings shall be analyzed and reported within the applicable annual period.<br>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents (PWS \ work definition \ task directive \ task assignment form, etc.), to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance. | ▪ No more than 4 violations per month.<br>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery. | ▪ CPARS assessment ratings.<br>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00. | Checklist and Customer Input |

| | | | | |
|---|---|---|---|---|
| Portfolio Services Deployment Deliverables and Tasks | ▪ 100% of on-going documentation and reporting of NITC Service Development milestone achievements shall be provided for new services proposed from the NITC Service Development Portal as defined by the NITC Service Development Lifecycle Directive.<br>▪ 100% attendance and active participation in all facilitation/collaboration/consultation events as required.<br>▪ 100% of facilitation/collaboration/consultation presentations and communications shall be coordinated as required and shall be clear, effective, concise, and organized.<br>▪ 100% of facilitation/collaboration/consultation activities shall be tailored specifically for subject matter needs and shall result in the team's ability and empowerment to achieve documented action items and milestones.<br>▪ 100% of documentation and services shall be completed and submitted IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance. | ▪ No more than 4 violations per month.<br>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery.<br>▪ Facilitation ineffectiveness may be determined to be a violation. | ▪ CPARS assessment ratings.<br>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00. | Checklist and Customer Input |

| | | | | |
|---|---|---|---|---|
| Documentation | ▪ 100% of all NITC Service Catalog documentation shall be produced and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings.<br>▪ 100% of all NITC Services Appendices documentation shall be produced, edited, reviewed, distributed and maintained, including the performance and documentation of required modifications/adds/deletes, to ensure accurate representation of NITC Service offerings.<br>▪ 100% of documentation shall be updated IAW the requirements established within the requirement documents, to include the required completion date and compliance with applicable governing regulations, directives, policies, procedures and guidance.<br>▪ Electronic versions of all documentation in the required format shall be posted/stored in the required artifact repository/tool location within the mutually established timeframe and shall be available for Government review at all times as required. | ▪ No more than 4 violations per month.<br>▪ Violations may include an error (including grammatical errors), omission, incorrect format, or delayed delivery. | ▪ CPARS assessment ratings.<br>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00. | Checklist and Customer Input |
| Weekly Status Report | ▪ 100% complete.<br>▪ 100% accurate.<br>▪ Submitted no later than (NLT) 2nd business day of the calendar week following the reporting period. | ▪ No more than 1 violation per month.<br>▪ A violation is an error (including grammatical errors), omission, or delayed delivery. | ▪ CPARS assessment ratings.<br>▪ Each additional violation beyond the AQL will result in a payment reduction of 3% up to the maximum reduction of $2,500.00. | Checklist and Customer Input |

| | | | | |
|---|---|---|---|---|
| Inquiry Response | ▪ Respond to all customer inquiries NLT 24 hours after inquiry receipt. | ▪ No more than 4 violations per month.<br>▪ A violation is an error (including grammatical errors), omission, or delayed delivery. | ▪ CPARS assessment ratings.<br>▪ Each additional violation beyond the AQL will result in a payment reduction of 1% up to the maximum reduction of $2,500.00. | Checklist and Customer Input |
| Security Incident Notification and Resolution | ▪ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).<br>▪ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be are addressed in accordance with Government direction. | ▪ No allowable violations per month. | ▪ CPARS assessment ratings.<br>▪ In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring. | Checklist and Customer Input |